УДК 004.056

Астахова Л. В.

ДОВЕРИЕ К КАДРОВОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация. В статье обоснована актуальность использования категории «доверие» к оценке кадровой безопасности информационной системы (ИС). Охарактеризованы ограничения к применению оценочных уровней доверия к кадровой безопасности информационной системы на основе ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Обоснован подход к оценке доверия к безопасности ИС за счет социотехнической сущности информационной системы и характеристик культурного капитала сотрудников и организации и выявления их отношения.

Ключевые слова: *доверие, кадровая безопасность, информационная безопасность, оценка, пользователь, информационная система.*

Astakhova L. V.

CONFIDENCE IN SECURITY PERSONNEL INFORMATION SYSTEM

In the article the urgency of using the category "trust" to the evaluation of personnel security information system (IS). Characterized by limiting the application of valuation levels of trust in the security of personnel information system based on ISO / IEC 15408-3-2013 Information technology. Methods and means of ensuring safety. Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Based approach to assessing the credibility of the IP security by socio-technical nature of the information system and the characteristics of the cultural capital of staff and the organization and identify their relationship.

Keywords: *trust, personnel security, information security, assessment, user information system.*

Введение. По данным отчета об утечках конфиденциальной информации за 2014 год Аналитического центра компании InfoWatch, по сравнению с 2013 годом, число утечек информации в мире выросло на 22%, в России – на 73%. В распределении утечек по регионам США традиционно занимают первую строчку по числу утечек (906), Россия заняла уже привычное второе место (167), на третьем месте - Великобритания (85). При этом в 71% случаев виновниками утечек информации были сотрудники компаний – настоящие или бывшие (69,2% и 1,4% соответственно) [1]. Эти цифры свидетельствуют о том, что пользователь (внутренний клиент) как важнейшее звено информационной системы серьезно недооценивается в практике обеспечения защиты информации, а сложившиеся в мире подходы к достижению доверия к безопасности информационных систем малоэффективны. Противоречие между ростом числа утечек информации по вине пользователей информационных систем, с одной стороны, и низкой эффективностью методик оценки доверия к их безопас-

ности – с другой, обусловливает актуальность проблемы доверия к пользователю информационной системы как ее неотъемлемой части, или – проблемы доверия к кадровой безопасности информационной системы.

Стандартный метод оценки доверия к информационной безопасности и его ограничения. Полагаем, что причина обоснованного противоречия - принципиальная сложность формализации процессов идентификации и оценки кадровых уязвимостей и рисков безопасности информационной системы (ИС) и попытки решить эти проблемы с позиций технико-технологических подходов. Один из таких подходов используется в стандарте ISO/IEC 15408-3:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components» [2] и идентичном ему ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» [3].

Традиционным способом достижения доверия является оценка (активное исследование) продукта информационных технологий (ИТ), который должен соответствовать определенным критериям безопасности. Названный стандарт выделяет 7 оценочных уровней доверия (ОУД) для оценки уровня доверия к объекту оценки (ОО). Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается заменой какого-либо компонента доверия иерархичным компонентом из того же семейства доверия (т.е. увеличением строгости, области охвата и/или глубины оценки) и добавлением компонентов из других семейств доверия (т.е. добавлением новых требований). Оценочный уровень доверия 1 (ОУД1) предусматривает функциональное тестирование; ОУД2 - структурное тестирование; ОУД3 - методическое тестирование и проверку; ОУД4 - методическое проектирование, тестирование и углубленную проверку; ОУД5 - полуформальное проектирование и тестирование; ОУД6 - полуформальную верификацию и тестирование проекта; ОУД7 - формальную верификацию проекта и тестирование [3]. Логично предположить, что в число компонентов доверия на разных оценочных уровнях следует включать: анализ Руководств различных категорий пользователей по эксплуатации; установление требований кадровой безопасности в задании по безопасности; анализ и обзор кадровых уязвимостей; тестирование кадрового обеспечения ИС; более всесторонний анализ кадровых уязвимостей и т.д.

Однако в контексте проблемы настоящей статьи описанная методика оценки доверия к информационной безопасности, закрепленная в международном стандарте, имеет существенные ограничения, которые выражаются в следующем.

Ограничение первое. Стандартная структура оценочных уровней доверия к безопасности ИС только на первый взгляд содержит потенциальные возможности для оценки кадровой безопасности. Пользователь как специфический объект оценки доверия в стандарте не упоминается. В теории и практике информационной безопасности этот вопрос также не разработан. Императив для преодоления этого ограничения: рассматривать в качестве объекта оценки доверия к информационной безопасности информационную систему как социотехническую систему.

Ограничение второе. Стандарт предлагает оценивать деятельность по достижению доверия к информационной безопасности, а не само доверие, которое выступает целью и результатом этой деятельности. Поскольку деятельность не всегда заканчивается достижением целей, валидность этой методики вызывает сомнения. Императив для преодоления этого ограничения: оценивать уровень доверия к самому пользователю, а не к деятельности по достижению доверия к нему. А это возможно только на основе гуманитарных подходов, которые позволяют изучить социокультурную обусловленность поведения человека.

Рассмотрим подробнее предлагаемые императивы преодоления ограничений стандартного метода оценки доверия к информационной безопасности для повышения его валидности.

Императив первый: социотехническая система как объект оценки доверия к информационной безопасности. Проблема доверия к неодушевленным предметам, к технике, к социотехническим системам активно исследуется сегодня в науке. Так, А.Б. Купрейченко обосновала основные структурные элементы модели доверия / недоверия к социотехническим системам: доверие / недоверие к принципам организации и правилам функционирования системы; доверие / недоверие к отдельным функциональным блокам (иерар-

хическим уровням, материально-технической базе, технологиям, отдельным узлам и элементам); доверие / недоверие к различным категориям людей, обеспечивающим функционирование системы (создателям, организаторам, модераторам системы и другим заинтересованным сторонам); доверие / недоверие к себе как профессионалу или пользователю; доверие / недоверие к условиям функционирования системы. В качестве основных детерминантов доверия / недоверия социальным и социотехническим системам автор называет личностные и социально-групповые факторы: базовое доверие / недоверие к миру, к другим людям, к себе, общее отношение к социальному и техническому прогрессу; интернальность, ответственность, склонность к риску, отношение к новизне и т. д. Кроме того, мы согласны с ученым и в том, что весомый вклад в проблему вносят культурно-исторические, социально-экономические и научно-технические факторы, в том числе культура доверия / недоверия в обществе и их уровень. [4., С.435 –436].

В основу системы оценки доверия к ИС как к социотехнической системе могут быть также положены три группы факторов, влияющие на организационное доверие, выделенные B. Uzzi:

• организационные факторы (характеристики организации) — структура, политика организации в отношении персонала, организационная культура;

• факторы отношений (характеристики ситуации) — первичное взаимодействие, ожидания, «стоимость обмена»;

• индивидуальные факторы (личностные характеристики субъекта доверия) — склонность к доверию, самоэффективность, ценности [5].

Нетрудно заметить, что перечень компонентов доверия к информационной системы как к социотехнической системе гораздо шире, чем идентичный перечень, представленный в стандарте ГОСТ Р ИСО/МЭК 15408-3-2013. Это подчеркивает специфику доверия к кадровой безопасности информационной системы и позволяет говорить о необходимости расширения критериев оценки доверия к ней в целом.

Императив второй: культурный капитал пользователя информационной системы как объект оценки доверия к информационной безопасности организации.

Анализ современных тенденций социально-экономической практики (парадигма «безопасность – через развитие»; культура информационной безопасности как императив для снижения рисков информационной безопасности; подход к человеку как к капиталу) позволил нам обосновать концептуальный подход к оценке кадровых рисков и уязвимостей на основе культурного капитала. Мы выделили в качестве объектов оценки индивидуальный и корпоративный культурный капиталы информационной безопасности.

Сущностью индивидуального культурного капитала информационной безопасности мы определили все культурные ресурсы индивида как получателя и отправителя информации в процессе информационного взаимодействия (базовые ценности, нормы, принципы, интеллектуальные, морально-нравственные и социальные качества, ценностно-ориентированные модели поведения), определяющие его способность к организации и развитию информационной деятельности и позволяющие ему получать дополнительные социально-экономические выгоды и легитимировать статусы, роли и власть.

Задача организации в процессе реализации цели обеспечения ее информационной безопасности – конвертировать сформированный индивидуальный культурный капитал информационной безопасности сотрудника (пользователя информационной системы) в корпоративный культурный капитал информационной безопасности. Под корпоративным культурным капиталом информационной безопасности мы понимаем все используемые организацией культурные ресурсы, которые накапливают сотрудники организации и организация в целом как отправители и получатели информации в процессе информационного взаимодействия, определяющие способность этой организации к развитию информационной деятельности и позволяющие организации получать дополнительные социально-экономические выгоды. Исследование проблем оценки культурного капитала активно ведется в современной экономической науке [6].

Исходя из определения понятий «культура информационной безопасности», «культурный капитал», «культурный капитал информационной безопасности организации», мы включили в структуру корпоративного культурного капитала информационной безопасности инкорпорированный, объективированный и институциональный культурные капиталы информационной безопасности. Каждый из них, в свою очередь, включает гуманистический и интел-

лектуальный капиталы. Обоснованный нами метод «отношений культурных капиталов» представляется весьма эвристичным для оценки доверия к кадровой безопасности информационной системы. Методика оценки кадровых уязвимостей информационной безопасности организации, основанная на выявлении индекса доверия как отношения культурных капиталов информационной безопасности индивида и организации, позволяет осуществлять мониторинг названных капиталов и разрыва между ними, оценивать необходимые направления развития структурного капитала организации для снижения рисков информационной безопасности в отношении каждого сотрудника в любой период времени. Подробнее об этом см. нашу публикацию [7, с.9].

Очевидно, что перечень выявленных компонентов доверия к кадровой безопасности организации в этом случае еще более обширен, чем идентичный перечень, представленный в стандарте ГОСТ Р ИСО/МЭК 15408-3-2013. Значительно превосходит он и перечень компонентов, обнаруженных в процессе социотехнического подхода к информационной системе. Это подчеркивает специфику доверия к кадровой безопасности информационной системы и позволяет говорить о необходимости расширения критериев оценки доверия к ней в целом.

Выводы.

Постоянный рост числа инцидентов информационной безопасности по вине персонала организации требует совершенствования методов оценки доверия к безопасности информационных систем за счет усиления их кадровой безопасности. Однако методика оценки доверия к безопасности информационной системы имеет существенные ограничения на ее использование в целях оценки доверия к кадровой безопасности информационной системы. Первое ограничение связано с игнорированием в стандартах социотехнического характера ИС, второе – культурно-капитальной сущности сотрудников (пользователей информационной системы) организации. В качестве императивов для снятия названных ограничений обосновано расширение компонентов доверия к безопасности информационной системы за счет: 1) социотехнических характеристик информационной системы и 2) характеристик культурного капитала сотрудников и организации в целом и их отношения. Адекватной мерой противодействия растущим объемам инцидентов информационной безопасности по вине сотрудников организации является разработка отдельного стандарта по оценке доверия к кадровой безопасности информационной системы.

Примечания

1. Глобальное исследование утечек конфиденциальной информации в I-м полугодии 2014 года. – URL: http://www.infowatch.ru/report2014_half (свободный, Загл. с экрана).

2. ISO/IEC 15408-3:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components» http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413

3. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – М.: Стандартинформ, 2014. –151 с.

4. Доверие и недоверие в условиях развития гражданского общества / отв. ред. А.Б. Купрейченко, И.В. Мерсияновой . – М.: Издательский дом НИУ ВШЭ, 2013. – 564 с.

5. Uzzi, B. Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness // Administrative Science Quarterly. – 1997. – Vol. 42. – No. 1. – P. 35–67.

6. Косьмина, Е.А., Метелев, С.Е., Косьмин, А.Д. Культурный капитал общества в реальном материале функционирующей организации. – М.: Экономика, 2007. – 386с.

7. Astakhova, L. V. Information Security: Risks Related to the Cultural Capital of Personnel (Review)// Scientific and Technical Information Processing, 2015, Vol. 42, No. 2, pp. 41–52.

Людмила Викторовна Астахова, доктор педагогических наук, профессор, профессор кафедры «Безопасность информационных систем» ФГБОУ ВПО «Южно-Уральский государственный университет». E-mail: lvastachova@mail.ru

Ludmila Astakhova, Doctor of Education, Professor, Department of Information Systems Security «South Ural State University». E-mail: lvastachova@mail.ru